International Journal of Security and Privacy in Pervasive Computing
Volume 13 • Issue 3 • July-December 2021

Scrambling Keypad for Secure Pin Entry to Defeat Shoulder Surfing and Inference Attacks

Samuel Selassie Yakohene, University of Ghana, Ghana

Winfred Yaokumah, University of Ghana, Ghana

https://orcid.org/0000-0001-7756-1832

Ernest Barfo Boadi Gyebi, University of Ghana, Ghana

ABSTRACT

Personal identification number (PIN) is a common user authentication method widely used especially for automated teller machines and point-of-sales devices. The user's PIN entry is susceptible to shoulder-surfing and inference attacks, where the attacker can obtain the PIN by looking over the user's shoulder. The conventional keypad with a fixed layout makes it easy for the attacker to infer the PIN entered by casual observation. This paper proposes a method of authentication to address these challenges. The paper develops a prototype numeric keypad with a layout akin to the conventional keypad, with the keys randomized for each PIN entry. The shuffle algorithm, Durstenfeld shuffle algorithm, is implemented in an application developed using JavaScript, which is a prototype-based object-oriented programming application that conforms to the ECMAScript specification. The prototype is implemented on three computing platforms for evaluation. The test proves the effectiveness of the system to mitigate shoulder-surfing and inference attacks.

KEYWORDS

Authentication, Durstenfeld Shuffle Algorithm, Fraud, Identity Theft, Inference Attacks, Personal Identification Number, Personal Information, Scrambling Keypad, Shoulder Surfing

DOI: 10.4018/IJSPPC.2021070102

INTRODUCTION

Most payment and banking services at both point of sale terminals (PoS) and automated teller machines (ATMs) are authenticated with the use of PINs (Nathaniel & Osuo-Genseleke, 2018). These applications are in public places where other people may be able to observe the process of keying in the PIN to authenticate the transaction. An adversary can easily gain access to the information by looking over one's shoulder to observe the process (Bošnjak & Brumen, 2019). Another way an adversary can obtain the information is through an inference attack (Kovelamudi, Zheng, & Mukkamala, 2017). This is done by observing the position and movement of the potential victim during the PIN entry process on the keypad. With the fixed positions for the keys on the standardized numeric keypad, it is not very difficult to accurately guess the digits of a PIN just by observing the login process. The attacker can gain access to the victim's financial information, be able to impersonate the victim to gain access to sensitive information or use the victim's identity to commit a crime. Scrambling keypad has been proposed to help overcome shoulder surfing and inference attack.

A scrambling keypad has a layout similar to a telephone keypad, but each time a key on the keypad is pressed the digits are scrambled to different positions other than the standard number positions (Phoka, Phetsrikran, & Massagram, 2018). This is to maintain optimum security such that when someone watching the PIN key-in process would not be able to determine the numbers being entered. The purpose of scrambling keypad is to prevent shoulder-surfing and inference attacks. Shoulder-surfing is a type of social engineering technique which attackers use to obtain information such as personal identification numbers, passwords and other confidential data by looking over the user's shoulder, either from keystrokes on a device or sensitive information being spoken (Hindusree & Sasikumar, 2015). Shoulder-surfing is a form of data theft where criminals steal a victim's personal information by observation the victim when using devices such as ATMs, computers, PoS terminals, and other electronics systems that require the use of a PIN for authentication (Kasat, Bhadade, & Trivedi, 2015). This can lead to identity theft or fraud. Evidence suggests that shoulder surfing occurs more frequently and can be easily carried out by an average user (Bošnjak & Brumen, 2019). Though it is quite safe when one is using a personal device in transactions that require an input of sensitive data, such as PINs on the numeric keypad, the issue of shoulder-surfing comes to play when using a public device or have to perform the transaction in a public place.

Inference attack is a data mining technique that is used to illegally access information about a subject or database by analyzing collected trivia data that is disclosed unknowingly. This is an example of breached information security where the attacker is able to deduce key or critical information of a database from trivial information, often through social engineering without directly accessing it (Turkanović, Družovec, & Hölbl, 2015). The most used mode of authentication is through the use of passwords and PINs (Kwon & Hong, 2015). The commonly used access control method is the password-based authentication, where the user inputs a pre-arranged